ORAL ARGUMENT NOT YET SCHEDULED

No. 24-5239

United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

IN RE: APPLICATION OF THE UNITED STATES
FOR AN ORDER PURSUANT TO 18 U.S.C. 2705(b)

Appeal from the U.S. District Court
for the District of Columbia
Case No. 1:24-mc-00058-JEB; Hon. James E. Boasberg

BRIEF OF INTERVENOR-APPELLANT

BRIAN J. FIELD
Counsel of Record
JOSHUA J. PRINCE
SCHAERR | JAFFE LLP
1717 K Street NW, Suite 900
Washington, DC 20006
(202) 787-1060
bfield@schaerr-jaffe.com

Counsel for Intervenor-Appellant

APRIL 4, 2025

CERTIFICATE AS TO THE PARTIES, RULINGS, AND RELATED CASES

Pursuant to Circuit Rule 28(a)(1), the undersigned counsel of record for Intervenor-Appellant Empower Oversight Whistleblowers & Research hereby provides the following information:

I. Parties, Intervenors, and *Amici* Appearing Below

The parties who appeared before the U.S. District Court were:

1. Empower Oversight Whistleblowers & Research, *Intervenor*; and

2. United States Department of Justice, *Plaintiff*.

The Government Accountability Project, Whistleblowers of America, and Michael German participated as *amici curiae* in the district court.

II. Parties, Intervenors, and *Amici* Appearing in this Court in this Matter

The parties and *Amici* who have appeared before the U.S. Court of Appeals for the District of Columbia Circuit in this matter are:

1. Empower Oversight Whistleblowers & Research, *Intervenor-Appellant*; and

2. United States of America, *Plaintiff-Appellee*.

To date, no *amici* have appeared in this Court.

Pursuant to Federal Rule of Appellate Procedure 26.1 and Circuit Rule 26.1, Intervenor-Appellant Empower Oversight Whistleblowers & Research ("Empower Oversight") submits the following corporate disclosure statement:

(a) Empower Oversight has no parent company, and there is no publicly held corporation holding 10% or more of its stock.

(b) Empower Oversight is a nonprofit, nonpartisan educational organization dedicated to enhancing independent oversight of government and corporate wrongdoing. Empower Oversight works to help insiders safely and legally report waste, fraud, abuse, corruption, and misconduct to the proper authorities, as well as work to hold authorities accountable to act on such reports.

III. Rulings Under Review

The ruling under review is the order entered on August 23, 2024, in the previously sealed matter *In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2705(b),* by the Honorable James E. Boasberg, U.S. District Court for the District of Columbia, granting in part and denying in part Empower Oversight's Motion to Unseal.

The Order and Memorandum Opinion are reprinted in the Appendix ("App.") at App.084 and App.085–092, respectively, filed concurrently with this brief.

IV. Related Cases

This case has not previously been filed with this Court or any other court. Counsel for Empower Oversight is not aware of any other related cases within the meaning of D.C. Circuit Rule 28(a)(1)(C).

/s/ Brian J. Field
Brian J. Field
Counsel for Intervenor-Appellant

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

*Authorities upon which we chiefly rely are marked with an asterisk.

Statutes

Rules

Other Authorities

GLOSSARY

ABBREVIATION	FULL NAME
DOJ	United States Department of Justice
Empower Oversight	Empower Oversight Whistleblowers & Research
NDO	Non-Disclosure Order
OIG	Office of the Inspector General, U.S. Department of Justice
The Act	Stored Communications Act

INTRODUCTION

In 2017, the Department of Justice ("DOJ") began issuing subpoenas to third-party providers to collect the communications records of members of Congress and congressional staff who were engaged in oversight of DOJ. DOJ hid these actions for more than six years by obtaining and annually renewing non-disclosure orders ("NDO") that prevented companies like Google from informing account holders that DOJ had subpoenaed their communications records, even years after DOJ had closed the underlying case it used to justify the subpoenas. Those subpoenas and NDOs present a host of serious concerns about DOJ's trampling on the constitutional separation of powers while concealing the true nature of its actions from the legislative and judicial branches.

It was not until 2023 when Jason Foster—the founder of Empower Oversight Whistleblowers & Research ("Empower Oversight")—learned DOJ had been hiding its collection of his and his Capitol Hill colleagues' communications records since 2017. Because DOJ collected records from the time when Mr. Foster was serving as Chief Investigative Counsel to the U.S. Senate Judiciary Committee, when he was routinely speaking

with executive-branch whistleblowers, DOJ could use the records to identify the whistleblower(s) with whom Mr. Foster spoke.

Considering the seriousness of DOJ's intrusion into these protected and confidential communications, Empower Oversight requested that the district court unseal DOJ's NDO applications. Those applications would provide important information to Mr. Foster, Congress, and the public about the extent to which DOJ complied with its own policies, the statute governing NDOs, and the separation of powers. Indeed, at the time of Empower Oversight's motion, it appeared likely that DOJ had failed to: (i) comply with the policies in the Justice Manual governing NDOs; (ii) disclose to the court sufficient information about the nature of the records collected to identify the separation of powers issues implicated; or (iii) identify specific facts to justify prohibiting Google from informing Mr. Foster that the executive branch had collected his legislative communications records. By withholding information, DOJ prevented the district court from being sufficiently informed about the underlying context to engage in meaningful review of the NDO requests.

Empower Oversight's suspicions have since been confirmed by an Inspector General investigation, which found that DOJ's NDO

applications failed to inform the district court about *any* key context surrounding the subpoenas—particularly failing to inform the court that DOJ obtained communications records from members of Congress and their staff who were actively engaged in oversight of DOJ. Rather, DOJ gave the court the false impression that these were routine subpoenas and NDO applications, providing only what the Inspector General called "boilerplate" explanations.

Unsealing the NDO applications in full will allow Congress and the public to judge for themselves whether the applications and the district court's review were consistent with the standards contemplated by the statute and DOJ policy or whether potential reforms are necessary. However, when the district court largely denied Empower Oversight's request to unseal the NDO applications, it failed to apply the common-law or the First Amendment rights of access, which exist to ensure exactly this sort of transparency.

Instead, the district court incorrectly relied on Federal Rule of Criminal Procedure 6(e) governing the confidentiality of grand jury proceedings, concluding that only scant portions of the NDO applications needed to be unsealed. Although the underlying subpoenas are related to

a grand-jury investigation, Rule 6(e) binds only government participants in the confidential proceedings, not third-party recipients of compulsory process. Third parties are normally free to discuss interactions with a grand jury absent court order, such as the NDOs obtained here pursuant to a process outlined in *statute*—not in Rule 6(e).

Because the district court erred at each turn, this Court should reverse and hold that Empower Oversight has common-law and First Amendment rights of access to the full, unredacted NDO applications, which will allow Mr. Foster and the public to learn precisely what DOJ stated to the court when asking for permission to force third parties like Google to keep the subpoenas secret for years.

JURISDICTION

Jurisdiction in the district court was based upon 28 U.S.C. § 1331. Jurisdiction in this Court is based upon 28 U.S.C. § 1291, as this appeal is from the final judgment of the district court and the related memorandum opinion and order, entered on August 23, 2024, by the Honorable James E. Boasberg, U.S. District Court for the District of Columbia, granting in part and denying in part Empower Oversight's

Motion to Unseal. Order and Memorandum Opinion, ECF Nos. 9 [App.0284] and 10 [App.085–092] (unpublished).

Notice of appeal was timely filed with the district court on October 10, 2024, and docketed in this Court on October 11, 2024.

ISSUES

1. Whether the district court erred in holding that Federal Rule of Criminal Procedure 6(e), rather than the common-law or First Amendment rights of access, governs Empower Oversight's motion to unseal.

2. Whether the district court erred in holding that the release of the withheld information would compromise grand-jury secrecy where the investigation had been widely reported.

RELEVANT STATUTES

Statutory authorities are included in the addendum to this brief.

STATEMENT

A. Statement of Facts

Jason Foster is the Founder of Empower Oversight. App.085. Before Empower Oversight, Mr. Foster served as Chief Investigative Counsel to the U.S. Senate Judiciary Committee. *Id.* In that role, Mr. Foster was responsible for directing congressional oversight

investigations into waste, fraud, abuse, and misconduct at DOJ, and he worked at the direction of the Committee's Chairman, Senator Chuck Grassley. App.010–011. As part of his work, Mr. Foster regularly spoke with whistleblowers, including executive branch employees, about government misconduct. App.012. In order to encourage whistleblowers to come forward, those conversations are expected to remain confidential.

In 2023, Mr. Foster received notice from Google that the company received a subpoena from DOJ in 2017 requiring Google to produce communications information associated with Mr. Foster's email address and two Google Voice telephone numbers, which were connected to his family's telephones and his official work phone at the U.S. Senate.[1] App.010. However, Google had been prohibited from informing Mr. Foster about the subpoena because DOJ obtained an NDO pursuant to 18 U.S.C. § 2705, along with annual renewals of the NDO each year until 2023. App.013–014.

[1] In addition to Mr. Foster's communications records, the subpoena required Google to produce records of other customers, including other congressional staffers, both Republicans and Democrats, who were also engaged in oversight of DOJ. App.012.

As was later confirmed, this subpoena—and others like it—related to an investigation DOJ conducted after the *New York Times* and the *Washington Post* published articles containing classified information.[2] After those articles were published, DOJ sought subpoenas for communications records of anyone who "had been provided, consistent with their job responsibilities, access to the classified information by the Department, a U.S. Intelligence Community agency, or another congressional staffer, or may have otherwise gained access to the information[.]" OIG Rep. 3. This led to subpoenas being issued to third parties for personal communications records of two members of Congress and 43 congressional staffers. *Id.* Conspicuously, there appears to be no evidence that DOJ sought records of *official*, congressionally provided phones or email accounts, either from the legislative branch itself or from third-party service providers.

---

[2] Off. Inspector Gen., U.S. Dep't of Just., No. 25-010, A Review of the Department of Justice's Issuance of Compulsory Process to Obtain Records of Members of Congress, Congressional Staffers, and Members of the News Media 1 (Dec. 2024) ("OIG Rep."), https://tinyurl.com/fnpjarsn. The Court can—and should—take judicial notice of this report under Federal Rule of Evidence 201(b), even though it was issued after the district court's order under review. *See Williams v. Lew*, 819 F.3d 466, 473 (D.C. Cir. 2016) (taking judicial notice of a government report cited in the "briefs, but not in the complaint").

Instead, DOJ broadly targeted *personal* telephone numbers and email addresses it believed belonged to legislative branch officials with no notice to the legislative branch. However, because of DOJ's overly broad approach, subpoenas included "phone number[s] or email address[es]" that were "not actually associated with the intended Member of Congress or staffer[.]" *Id.* at 28. In one instance, the subpoena "returned subscriber information for the Member's spouse and child."[3] *Id.*

For these subpoenas, DOJ required Google to release customer or subscriber information, as well as the subscribers' names, addresses, local and long-distance telephone connection records, text message logs, records of session times and durations, length of service, and types of service utilized for the period from December 1, 2016, to May 1, 2017 ("communications records"). App.045–046. The subpoena therefore compelled the release of detailed logs about Mr. Foster's communications, indicating with whom, precisely when, how often, and for how long Mr.

[3] Among others, this includes Kashyap Patel, currently the Director of the Federal Bureau of Investigation and formerly a staffer at the U.S. House of Representatives Permanent Select Committee on Intelligence ("HPSCI"). Around this same time, Deputy Attorney General Rosenstein had threatened to subpoena HPSCI staffers' personal records during a confrontation over DOJ's refusal to comply with that committee's compulsory process. App.012.

Foster was communicating. Given Mr. Foster's role as Chief Investigative Counsel, this meant DOJ compelled Google to provide it with information that would easily enable DOJ to identify confidential whistleblowers who were providing Congress with information about government misconduct.

This raised serious concerns about DOJ's intrusion into the separation of powers, leading to an Inspector General investigation. As the Inspector General report explains: "[DOJ's] decision to compel the production of non-content communications records of Members of Congress and congressional staffers implicated the constitutional rights and authorities of a co-equal branch of government." OIG Rep. 3. Indeed, the subpoenaed information "can reveal the fact of sensitive communications of Members of Congress and staffers, including with executive branch whistleblowers and with interest groups engaging in First Amendment activity." *Id.* at 4.

That is troubling on its own. But the OIG also confirmed that DOJ withheld this key context from Google and the district court when requesting the subpoenas and NDOs. Instead, the OIG concluded—after reviewing the still-sealed NDO applications at issue here, among

others—that DOJ "relied on general assertions about the need for non-disclosure rather than on case-specific justifications." *Id.* In fact, by August 2021, when DOJ sought the fourth NDO extension, DOJ's NDO renewal applications *still* "contained the same boilerplate assertions" as the initial application and *still* "did not reference[] the fact that they related to requests for records of Members of Congress or congressional staffers." *Id.* Rather, when explaining the need for the NDO, DOJ relied on "general language describing the risks that could arise if the compulsory process was disclosed[.]" *Id.* at 41.

DOJ thus not only relied on these vague descriptions at the outset of its investigation, but continued to do so for years—even after the leak investigation led to the 2018 guilty plea from Former Senate Intelligence Committee Security Director James Wolfe for lying to the FBI about his media contacts. *Id.* at 43 n.114.[4]

[4] *See also Empower Oversight Obtains Copies of Google Gag Orders, Presses Justice Department to Justify Hiding its Collection of Congressional Staff Communications Records from the Public*, Empower Oversight Whistleblowers & Rsch. (Dec. 4, 2023), http://tinyurl.com/57h5d3m4; Adam Goldman et al., *Ex-Senate Aide Charged in Leak Case Where Times Reporter's Records Were Seized*, N.Y. Times (June 7, 2018), http://tinyurl.com/yfac9pxs.

Moreover, even now that the NDOs have expired and all underlying "investigations are now closed," DOJ still refuses to allow Empower Oversight and the public to see the explanations DOJ provided the court when obtaining the NDO for the subpoena seeking Mr. Foster's records. OIG Rep. 3. And, by largely denying Empower Oversight's request to unseal the NDO applications, the district court has kept those applications hidden *even after* the underlying cases have been closed.

Thus, Congress and the public are prevented from scrutinizing the claims made by DOJ and accepted by the district court that supposedly justified gag orders under these extraordinary circumstances to prevent Google from notifying its legislative branch customers of the subpoenas even long after-the-fact.

B. Procedural History

On May 2, 2024, Empower Oversight filed a motion to intervene and for unsealing of the motions DOJ filed in support of its NDO applications. App.002–034. As Empower Oversight explained in that motion, the public has a vital interest in understanding the explanations DOJ provided the court when requesting that the court prohibit Google from informing anyone, including congressional leadership, Mr. Foster,

or the other targeted congressional staff, about the underlying subpoena for more than six years.

On June 20, 2024, DOJ opposed Empower Oversight's request to intervene and its request for unsealing. App.051–059. In addition to its opposition brief, DOJ filed a sealed *ex parte* addendum in support of its opposition. Dist. Ct. ECF No. 6 [under seal]. Empower Oversight filed its reply brief on July 15, 2024. App.060–083.

On August 23, 2024, the district court granted Empower Oversight's motion to intervene, and the court partially granted Empower Oversight's motion to unseal, ordering DOJ to unseal the "typical jurisdictional discussion" from "the initial [NDO] application." App.089. However, the district court held that the remaining portions of the applications "must stay [under seal] and that releasing applications beyond the [redacted] initial application to extend the NDO is unwarranted." *Id.*

On September 3, 2024, DOJ provided Empower Oversight with the redacted copies of the first NDO application and one renewal request. App.093–097, 098–103. The key portions of the applications, however,

remain sealed, and the key applications approved after the underlying investigation concluded remain sealed. *Id.* This appeal timely followed.

SUMMARY OF ARGUMENT

The district court should have granted Empower Oversight's motion to unseal the full NDO applications. Those applications are judicial records containing the arguments DOJ made to influence the district court's decision to impose a prior restraint on third-party speech under specific, limited circumstances proscribed by statute. Accordingly, the applications are subject to common-law and First Amendment rights of access. They are not grand jury materials subject to Rule 6(e).

1. Empower Oversight has a common-law right of access to the NDO applications. The district court erred in concluding instead that the NDO applications are ancillary grand-jury materials such that Rule 6(e) governs and forbids their disclosure "as long as necessary to prevent the unauthorized disclosure of a matter occurring before a grand jury." The applications, which sought to influence the district court, are judicial records, not grand-jury materials.

This straightforward conclusion is underscored by the fact that NDO applications are authorized by, and creatures of, the Stored

Communications Act, a statute that provides its own standard for confidentiality. *See* 18 U.S.C. § 2705(b). It is a fundamental rule of statutory interpretation that specific statutes control over general ones, and that rule applies with full force here. *Gozlon-Peretz v. United States*, 498 U.S. 395, 407 (1991). Because § 2705(b) speaks more specifically to the documents Empower Oversight seeks than does Rule 6(e), § 2705(b) provides the governing standard. And, by any reading of that statute, the time for secrecy under § 2705(b) expired when DOJ elected to let the NDOs expire. Accordingly, Empower Oversight has a common-law right of access to the NDO applications, and this Court should apply the six-factor test for unsealing judicial records established in *United States v. Hubbard*, 650 F.2d 293 (D.C. Cir. 1980).

Furthermore, even if the district court were correct that the NDO applications are ancillary grand-jury materials, the Inspector General report and related publicity of the investigation demonstrates that there is no longer any need "to prevent the unauthorized disclosure of a matter occurring before a grand jury." Fed. R. Crim. P. 6(e)(6). Indeed, as this Court's cases recognize, the time comes when even ancillary grand-jury materials can be released. *See In re North*, 16 F.3d 1234, 1245 (D.C. Cir.

1994). A public report detailing DOJ's investigation, and explaining the substance of the NDO applications, surely fits the bill. The NDO applications should thus be unsealed even if this Court agrees with the district court that they are ancillary grand-jury materials.

2. Alternatively, Empower Oversight has a First Amendment right of access to the NDO applications, and DOJ's attempt to keep them sealed cannot survive strict scrutiny. Under the applicable "experience and logic" test, the First Amendment is implicated when (a) the types of judicial processes or records sought have historically been available to the public, and (b) public access plays a "significant positive role" in the functioning of those processes. *See Press-Enter. Co. v. Superior Court*, 478 U.S. 1, 9, 11 (1986). And when experience and logic support a First Amendment right, strict scrutiny applies.

Here, both experience and logic confirm a First Amendment right of access to the NDO applications. As for experience, there is a long tradition of providing access to documents filed in connection with prior restraint proceedings, even where the information involves matters of national security. And though Congress could have automatically required that all subpoenas issued under the Stored Communications Act

be kept confidential, it did not do so. As for logic, providing access to the NDO applications will allow for greater public scrutiny of DOJ's activities, and the Supreme Court has recognized that such scrutiny is an important check on the government. *See Nixon v. Warner Commc'ns, Inc.*, 435 U.S. 589, 597–98 (1978).

Because the First Amendment applies, DOJ's desire to keep the NDO applications under seal is subject to strict scrutiny, which it cannot survive. DOJ lacks a compelling interest in keeping its investigation secret after that investigation has been the subject of a public Inspector General report and has long been closed. And DOJ cannot show that its sealing of the NDO applications is narrowly tailored.

STANDARD OF REVIEW

This Court reviews "de novo a district court's determination" about whether "a document is a judicial record" and whether the district court "applied the proper legal standard." *Cable News Network, Inc. v. Fed. Bureau of Investigation*, 984 F.3d 114, 117 (D.C. Cir. 2021) (cleaned up). Unsealing orders are otherwise reviewed for abuse of discretion. *Id.*

ARGUMENT

Empower Oversight has a common-law and First Amendment right of access to the NDO applications. The district court erred when it concluded that Rule 6(e) applies and precludes unsealing the key portions of the NDO applications.

I. The Common-Law Right of Access to Judicial Records Requires Unsealing the NDO Applications.

In this Circuit, "[t]he presumption of openness in judicial proceedings is a bedrock principle of our judicial system." *In re Sealed Case*, 971 F.3d 324, 325 (D.C. Cir. 2020). Because this presumption "stems from the general public interest in the openness of governmental processes, and, more specifically, from the tradition of open judicial proceedings[,]" that presumption is "customary and constitutionally embedded[.]" *In re Sealed Case*, 931 F.3d 92, 96 (D.C. Cir. 2019) (cleaned up). And, where the records in question are "judicial records," the common-law right of access applies, and courts must consider public disclosure under this Court's *Hubbard* test. *United States v. Hubbard*, 650 F.2d 293 (D.C. Cir. 1980).

The district court erred in failing to apply these principles, concluding instead that the NDO applications were ancillary grand-jury

materials subject to Rule 6(e). But NDO applications are plainly not ancillary grand-jury matters—they are creatures of the Stored Communications Act, which this Court has already held "contains no default sealing or nondisclosure provisions." *In re Leopold to Unseal Certain Elec. Surveillance Appls. & Ords.*, 964 F.3d 1121, 1129 (D.C. Cir. 2020) ("*Leopold II*") (cleaned up). However, even if the records are ancillary grand-jury materials, the district court nonetheless erred in failing to order their full unsealing.

A. NDO applications are judicial records.

This Court has previously held that Stored Communications Act subpoenas and related applications are judicial records. *Leopold II*, 964 F.3d at 1128. And, for judicial records, the common-law right of access applies unless a statute expressly sets the terms for public access. *Id.* at 1129. The district court incorrectly concluded that the NDO applications authorized by 18 U.S.C. § 2705(b) are ancillary grand-jury materials such that the common-law right of access did not apply.

1. The NDO applications are judicial records. As this Court has explained, while "not all documents filed with courts are judicial records," court orders related to electronic surveillance are judicial records, as are

"applications for such orders and their supporting documents." *Leopold II*, 964 F.3d at 1128. This Court further explained that the relevant question is whether documents filed are "intended to influence" a court. *Id.* If a court may have relied on a party's submission in making a substantive ruling, "that is more than enough to make them judicial records." *MetLife, Inc. v. Fin. Stability Oversight Council*, 865 F.3d 661, 668 (D.C. Cir. 2017).

Here, the NDOs are authorized by 18 U.S.C. § 2705(b). Under that provision, a "governmental entity … may apply to a court for an order commanding a provider of electronic communications service … to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." 18 U.S.C. § 2705(b). Continuing, that provision instructs courts to issue the NDO if the requesting entity shows that notification about the subpoena "will result" in one of several listed harms (*e.g.*, endangering life, flight from prosecution, destruction of evidence). *Id.* Thus, an NDO application must identify the specific harm that "will result" from notification, and the

application must provide the court with information to use when determining the "appropriate" duration for the NDO.

Accordingly, the NDO applications were clearly intended to influence the court's decision making, and that is "more than enough" to make them judicial records. *MetLife*, 865 F.3d at 668.

2. Because the applications are judicial records, the common-law right of access applies by default unless "Congress has spoken directly to the issue at hand." *Leopold II*, 964 F.3d at 1129. Here, the district court concluded that Rule 6(e) applied and supplanted the common-law right of access. Not so.

DOJ relied on the Stored Communications Act (the "Act") when requesting the NDOs. *See* App.093, App.098. In *Leopold II*, this Court considered a similar question—whether the Act expressly addresses access and displaces the common-law right of access. This Court explained that, although the Act authorizes courts to issue warrants and orders under 18 U.S.C. § 2703(d), the Act does not *automatically* "require the sealing of warrants or § 2703(d) orders and applications in support thereof." *Leopold II*, 964 F.3d at 1129. Rather, the Act only authorizes the government to seek a "separate order prohibiting the service provider

from notifying anyone about the electronic surveillance order, 'for such period as the court deems appropriate[.]'" *Id.* (quoting 18 U.S.C. § 2705(b)). Thus, because the Act does not contain a "default sealing or nondisclosure provision[]," the Court concluded that "the common-law rule applies."[5] *Leopold II,* 964 F.3d at 1129.

The *Leopold II* Court then contrasted orders issued under the Act with both pen register orders and Rule 6(e) materials, explaining that, unlike the Stored Communications Act, the Pen Register Act requires a pen register order to "direct that … the order be sealed until otherwise ordered by the court." *Id.* at 1130 (quoting 18 U.S.C. § 3123(d)(1)). Congress thus "expressly direct[ed] sealing" for pen register orders and therefore "displaced the usual presumption in favor of access." *Id.* Similarly, as to Rule 6(e) materials, *Leopold II* explained that Congress again "expressly directs secrecy as the default position, [which] thus displaces the common-law right of access." *Id.* That is because Rule 6(e) lists several grand-jury-related records that "must be kept under seal to

[5] The only other Circuit to address this question agrees. *See In re U.S. for an Ord. Pursuant to 18 U.S.C. Section 2703(D)*, 707 F.3d 283, 291 (4th Cir. 2013) ("Because we conclude that § 2703(d) orders are "judicial records," the common-law presumption of access attaches to these documents.").

the extent and as long as necessary to prevent the unauthorized disclosure of a matter occurring before a grand jury." *Leopold II*, 964 F.3d at 1130 (quoting Fed. R. Crim. P. 6(e)(6)). For *those* records, Congress established a test through Rule 6(e).

By contrasting documents prepared under the Stored Communications Act with Rule 6(e), the *Leopold II* Court concluded that judicial records prepared pursuant to the Act are *not* Rule 6(e) materials. 964 F.3d at 1129–30. And *Leopold II* did not find that Stored Communications Act warrants and § 2703(d) orders issued during criminal investigations fell under Rule 6(e)'s purview—even though such information could certainly be used in grand-jury investigations. 964 F.3d at 1129. Rather, the Court explained that the common-law right of access is "fundamental," and the Court directed the district court to apply the common-law rules on remand to determine "how and when greater access can be provided." *Id.* at 1130, 1135.

This Court should do likewise. The Act permits the government to "seek a separate order prohibiting the service provider from notifying anyone about the electronic service order, 'for such period as the court

deems appropriate[.]'" *Id.* at 1129 (quoting 18 U.S.C. § 2705(b)). Of course, once such an NDO expires, the Act no longer supports secrecy.

As the Inspector General explained, the investigations underlying the subpoenas and NDOs "are now closed[.]" OIG Rep. 3. And, once those investigations ended, DOJ itself allowed each of the resulting NDOs from the requested applications to expire, *id.* at 42 n.111, finally allowing Google to inform Mr. Foster of the production of his communications records. Accordingly, there no longer exists a need "to protect specified law enforcement interests in connection with ongoing investigations." *Leopold II*, 964 F.3d at 1129 (citing 18 U.S.C. § 2705(b)). And that conclusion flows directly from DOJ's decision to allow the orders to expire without seeking additional extensions. Accordingly, the common-law right of access applies to the NDO applications.

3. In contrast, Rule 6(e)(6) expressly applies to "[r]ecords, orders, and subpoenas" that relate to grand-jury proceedings when revealing those documents could "disclos[e] [] a matter occurring before a grand jury." *Id.* Because the rule is expressly limited to a narrow subset of records, this Court has explained that it falls far short of "draw[ing] 'a veil of secrecy ... over all matters occurring in the world that happen to

be investigated by a grand jury.'" *Senate of the Commw. of P.R. on Behalf of Judiciary Comm. v. U.S. Dep't of Just.*, 823 F.2d 574, 582 (D.C. Cir. 1987) (quoting *SEC v. Dresser Indus., Inc.*, 628 F.2d 1368, 1382 (D.C. Cir. (1980) (en banc)). And this Court further rejected a "*per se* rule against disclosure of any and all information which has reached the grand jury chambers." *Id.* Indeed, "[t]he mere fact that information has been presented to the grand jury does not itself permit withholding." *Labow v. U.S. Dep't of Just.*, 831 F.3d 523, 529 (D.C. Cir. 2016).

Instead, the "touchstone" for determining Rule 6(e)'s applicability is whether revealing a document would lead to a discovery of the "grand jury's identity, investigation, or deliberation." *Id.* Information that is "coincidentally before the grand jury which can be revealed in such a manner that its revelation would not elucidate the inner workings of the grand jury is not prohibited." *In re Sealed Case No. 99-3091*, 192 F.3d 995, 1002 (D.C. Cir. 1999) (per curiam) (cleaned up). And this Court has clarified that where "reported deliberations do not reveal that an indictment has been sought or will be sought, ordinarily they will not reveal anything definite enough to come within the scope of Rule 6(e)." *Id.* at 1003 (emphasis omitted).

The NDO applications are not remotely analogous to the grand-jury materials that this Court has held are protected by Rule 6(e). Unlike plaintiffs in *In re Sealed Case*, Empower Oversight did not seek the "mandatory public docketing of grand jury ancillary proceedings." *In re Sealed Case*, 199 F.3d 522, 525 (D.C. Cir. 2000). Nor did Empower Oversight seek access to the grand jury subpoena (which it already had), any "objections to the grand jury subpoena," "hearings" pertaining to such objections, or "access to any hearings, and transcripts of such hearings" that took place before the grand jury. *In re Motions of Dow Jones & Co.*, 142 F.3d 496, 499 (D.C. Cir. 1998).

DOJ thus cannot seriously contend that the NDO applications will "elucidate the inner workings of the grand jury" beyond what has already been revealed by the disclosure of the subpoena itself or the subsequent Inspector General report. *In re Sealed Case No. 99-3091*, 192 F.3d at 1002. Nor is it likely that the NDO applications would have shown that "an indictment *has been* sought or *will be* sought," *id.* at 1003, as the NDO

applications were presented not to the grand jury but to the district court to prevent the disclosure of DOJ's investigation.

Moreover, whatever risk of unauthorized disclosure there may have been earlier, the Inspector General has put such concerns to rest by explaining that DOJ closed its investigation without charging anyone with disclosing classified information. OIG Rep. 3. To treat the NDO applications as grand-jury materials on these facts would be to dramatically expand the category of records historically treated as ancillary grand-jury materials.

B. Applying the *Hubbard* test, this Court should unseal the NDO applications.

Because the common-law right of access applies, the district court should have applied the six-part *Hubbard* test, which requires the court to consider the following factors:

> (1) the need for public access to the documents at issue;
> (2) the extent of previous public access to the documents;
> (3) the fact that someone has objected to disclosure, and the identity of that person;
> (4) the strength of any property and privacy interests asserted;
> (5) the possibility of prejudice to those opposing disclosure; and
> (6) the purposes for which the documents were introduced during the judicial proceedings.

MetLife, Inc., 865 F.3d at 665 (citing *Hubbard*, 650 F.2d 293, 317–22). Under this test, the burden for demonstrating the need for sealing lies with the government, which must show that "disclosure will work a clearly defined and serious injury[.]" *In re Cendant Corp.*, 260 F.3d 183, 194 (3d Cir. 2001) (quoting *Miller v. Indiana Hosp.*, 16 F.3d 549, 551 (3d Cir. 1994)). Because the district court incorrectly held that Rule 6(e) applied, it failed to apply these factors. When applied, the balance of interests unequivocally supports disclosure.

1. The public has a strong interest in the NDO applications.

As to the first factor, which considers the need for public access to the requested documents, the public has a strong interest in learning more about DOJ's collecting communications records belonging to those entrusted with congressional oversight. The public also has an equally compelling interest in learning about DOJ's demands to keep its tactics secret. *See Nixon*, 435 U.S. at 597–98 ("The interest necessary to support the issuance of a writ compelling [public] access has been found, for example, in the citizen's desire to keep a watchful eye on the workings of public agencies[.]"); *FTC v. Standard Fin. Mgmt. Corp.*, 830 F.2d 404, 410 (1st Cir. 1987) ("The appropriateness of making court files accessible is

accentuated in cases where the government is a party: in such circumstances, the public's right to know what the executive branch is about coalesces with the concomitant right of the citizenry to appraise the judicial branch."). This public interest has only increased with the recent publication of the Inspector General's report, which discusses DOJ's various missteps in how it investigated its overseers. *See generally* OIG Rep.; Editorial, *When the Justice Department Spied on Congress*, Wall Street J. (Oct. 26, 2023), http://tinyurl.com/3bun3ft3.

As to the subpoenas themselves, the public has a keen interest in understanding why DOJ intruded into both the personal and official activities of attorneys advising congressional committees overseeing the Department. This implicates serious issues of public interest, including the separation of powers, Legislative Branch privilege, and the protection of the identity of confidential whistleblowers whose assistance to the American people's elected representatives is essential to the constitutional oversight of the Executive Branch.

As to the NDO applications, the public also has an interest in learning about DOJ's candor with the court regarding the nature of the underlying subpoenas. Without such information, the public is left to

assume DOJ was seeking to conceal its overly broad approach to the communications records of congressional Members and staff in order to avoid public scrutiny. And, if DOJ was less than candid about the nature of the underlying subpoenas, that would have prevented the district court from engaging in the fully informed, critical review of the NDO requests intended by the statute. As noted earlier, § 2705(b) identifies the specific factual details DOJ must include in an NDO application and the specific findings a court must make before issuing an NDO. *See* 18 U.S.C. § 2705(b) (DOJ must provide facts allowing the district court to find that "notification of the existence of the warrant, subpoena, or court order *will result* in" one of the listed harms (emphasis added)).

However, the Inspector General has now confirmed that each successive NDO application relied instead on the same "boilerplate" objections to disclosure. OIG Rep. 4. The public undoubtedly has an interest in learning more about these explanations, as that information bears on the sufficiency of DOJ's explanations and on the district court's

analysis of the NDO applications.[6] And, even if DOJ sought to keep its dragnet subpoena secret for other reasons, the public has a right to know.

Further, the public has a "strong interest in reviewing documents 'specifically referred to in the trial judge's public decision[.]'" *Vanda Pharms. Inc. v. Food & Drug Admin.*, 539 F. Supp. 3d 44, 52 (D.D.C. 2021) (quoting *Hubbard*, 650 F.2d at 318). Because the lower court's NDOs have now expired, they are in the public domain. *See* App.035–043. Accordingly, "the public also has a transparency interest in knowing what record evidence the Court saw fit to exclude [as well as include] from its explanation of the reasons underlying its ultimate decision." *Vanda Pharms.*, 539 F. Supp. 3d at 53 (citing *MetLife*, 865 F.3d at 668).

2. Previous public access to the records requires disclosure.

The second factor looks to whether the requested materials have previously been disclosed to the public and supports unsealing. As courts in this Circuit have recognized, "[i]f members of the public already have had access to the Challenged Documents, there would presumably be less

[6] Similarly, the public has an interest in seeing these applications to render its own conclusion about whether the Inspector General's conclusions are accurate.

justification to keep them under seal." *Vanda Pharms.*, 539 F. Supp. 3d at 54. Here, several of the subpoenas to which the NDOs relate have been publicly released. Moreover, the NDO applications themselves have been discussed at length by the Inspector General. Thus, this factor weighs in favor of unsealing the materials. *See In re Appl. of N.Y. Times Co. for Access to Certain Sealed Ct. Recs.*, 585 F. Supp. 2d 83, 93 (D.D.C. 2008) (holding that when "critical information is already in the public forum ... this factor weighs in favor of unsealing the ... materials").

But even if this Court considers the disclosures of the underlying subpoenas irrelevant to its consideration of the public's access to the NDO applications, it should—at most—consider this factor neutral. In *Hubbard*, after the Court found that there was "no such access to the documents" sought, the Court explained that there was "no previous access to weigh in favor" of unsealing. *Hubbard*, 650 F.2d at 318–19.

3. DOJ's objection to unsealing is outweighed by the other factors.

To the extent DOJ continues to resist any further unsealing of the NDO applications, it overlooks several countervailing facts: (1) the underlying subpoena is already public; (2) the Inspector General stated that the applications do not include any case-specific information; and

(3) the underlying investigations are closed. While DOJ's continued opposition concededly weighs against disclosure, this Court should afford it little weight because each of the other factors so clearly favors unsealing the NDO applications. *See EEOC v. Nat'l Children's Ctr., Inc.*, 98 F.3d 1406, 1410 (D.C. Cir. 1996) (reversing a decision to seal documents when the only factor weighing in favor of sealing was the other party's objection).

4. The NDO applications implicate minimal privacy interests.

As to the fourth factor, there is no reason to conclude that appropriately redacted documents would jeopardize anyone's property or privacy interests. As Empower Oversight explained below, it has no objection to the redaction of specific names. *See* App.010 n.1. With names redacted, DOJ cannot credibly argue that releasing the applications will reveal the names of those it targeted.

Moreover, considering the Inspector General's conclusion that both the "original and renewal" applications lacked any "case-specific justifications," and instead relied on "the same boilerplate assertions about the need for non-disclosure," it is highly unlikely that any further identifying information was included in the NDO applications. OIG

Rep. 44. However, even where such interests are implicated, courts in this Circuit explain that "this factor does not serve as a blanket excuse to keep the public from accessing entire judicial records[.]" *Vanda Pharms.*, 539 F. Supp. 3d at 55 (citing *Hubbard*, 650 F.2d at 324). The fourth factor thus weighs in favor of disclosure.

5. DOJ will not be prejudiced by unsealing.

The fifth factor likewise weighs in favor of disclosure, as DOJ has allowed the NDOs to expire, having determined that information relating to the subpoena no longer must be kept secret.

Indeed, DOJ clearly faces no prejudice, as the underlying "investigation is complete and therefore is not in danger of being thwarted if the Court releases the documents." *Appl. of N.Y. Times*, 585 F. Supp. 2d at 93. Moreover, the Inspector General has released its report that publicly discusses the details of the investigations that led to the subpoena, meaning that the public already knows many details about the government's investigation.

Nor is there a risk that disclosing the government's NDO applications will reveal new information about that investigation. Here again, the Inspector General found that the "NDO applications filed with

the courts—both in original and renewal applications—relied on general assertions about the need for non-disclosure rather than on case-specific justifications." OIG Rep. 4. DOJ cannot show harm from the public's learning what "boilerplate assertions about the need for non-disclosure" DOJ used when seeking to collect communications of members of Congress and their staffers. *Id.* at 44. Since such generalized, boilerplate assertions about the need for non-disclosure will be the same assertions given in any case, DOJ can safely release them here.

6. The purpose of the NDO applications supports disclosure.

Finally, the purpose for which the applications were filed strongly supports unsealing. This factor favors disclosure when "the parties explicitly intended the Court to rely on [the sealed] materials in adjudicating their dispute." *Berliner Corcoran & Rowe LLP v. Orian*, 662 F. Supp. 2d 130, 135 (D.D.C. 2009). As this Court has explained, "[w]hen a sealed document is considered as part of judicial decisionmaking, the sixth factor will oftentimes carry great weight.'" *Cable News Network*, 984 F.3d at 120; *accord Hubbard*, 650 F.2d at 321 (calling the sixth factor the "single most important" on the facts before it).

The documents in question were undoubtedly "part of judicial decision making," because the district court necessarily considered them when determining whether to issue NDOs. As this Court explained in *Leopold II*, "the [Stored Communications Act] contains no default sealing or nondisclosure provisions," *Leopold II*, 964 F.3d at 1129, meaning that the lower court here could not have prevented the disclosure of the subpoena unless the government first "appl[ied] to [the] court for an order commanding" Google "not to notify" its customers "of the existence of the … subpoena[,]" 18 U.S.C. § 2705(b). By asking the Court to forbid Google from informing its customers about the subpoena, DOJ sought to ensure that the subpoena would not be challenged or subject to an objection from the relevant customers. Here, those customers were exclusively legislative branch officials exercising constitutional oversight of DOJ, a fact DOJ concealed from Google and apparently from the district court. The sixth *Hubbard* factor thus weighs heavily in favor of disclosure.

Moreover, DOJ's main purpose in requesting the NDOs—to prevent disclosure of the subpoenas and related investigation—is now moot several times over. The NDOs have expired, the underlying subpoenas and investigation have been disclosed, and the underlying case is long

closed. The Inspector General has also publicly reported on the subpoenas, the applications, and the NDOs. Thus, whether this factor is viewed solely as a question of whether DOJ's purpose was to influence the court or whether this Court considers its main purpose—preventing disclosure—this final *Hubbard* factor supports disclosure.

C. Even if the NDO applications are ancillary grand-jury materials, they must be unsealed.

If this Court concludes instead that the NDO applications are subject to Rule 6(e)(6), the Court should still reverse the district court because the grand jury matter has now been widely reported, and there is no basis for continuing to keep them sealed following the Inspector General's report.

The district court held that the publicity concerning the government's activities here was "dramatically less" than the publicity in other cases and—on that basis alone—declined to unseal the records under the publicity exception. App.091. But the publicity in other cases differed from the publicity here only in degree, not kind. It remains true that the underlying investigation was public, and it has only become more public through the Inspector General report.

Rule 6(e) is designed to "preserve secrecy." Accordingly, this Court has recognized that there "come[s] a time … when information is sufficiently widely known that it has lost its character as Rule 6(e) material." *In re North*, 16 F.3d at 1245. When a party seeks documents relating to matters that "have already been publicly disclosed," "[c]ourts may unseal records containing matters occurring before a grand jury." *In re Cheney*, No. 23-5071, 2024 WL 1739096, at *3 (D.C. Cir. Apr. 23, 2024) (per curiam).

Applying those standards, the district court clearly erred in concluding that the grand jury investigation was not sufficiently known at the time of Empower Oversight's motion. As already shown, Empower Oversight did not learn about the investigation until several years after it ended. Indeed, even after DOJ had stopped investigating, it continued to seek extensions of the NDO. But once the NDOs expired, Google notified Mr. Foster that DOJ had subpoenaed his Google records and gave him a copy of the subpoena. Google also informed Mr. Foster that the government had forbidden it from informing him about the subpoena—by giving him the NDOs.

Thus, when Empower Oversight sought to unseal the applications, it already possessed the subpoena and the NDOs. *See* App.035–047. Because the subpoena and the NDOs were "part of the public record," the government cannot claim a need to keep the investigation secret. *In re Grand Jury Subpoena, Judith Miller*, 438 F.3d 1138, 1140 (D.C. Cir. 2006) (per curiam). Moreover, DOJ previously announced its own investigation into the Department's subpoena abuses.[7] And DOJ acknowledged the indictment that the grand jury returned following its investigation into the press leaks.[8]

---

[7] Off. of Inspector Gen., U.S. Dep't of Just., *Ongoing Work, Review of the Department of Justice's Use of Subpoenas and Other Legal Authorities to Obtain Communication Records of Members of Congress and Affiliated Persons, and the News Media*, https://tinyurl.com/2s4vmmba (snapshot of the Inspector General's website from June 28, 2024, showing OIG's then-pending investigation into DOJ's "use of subpoenas and other legal authorities to obtain communication records of Members of Congress and affiliated persons" as "Ongoing Work").

[8] Press Release, U.S. Att'y's Off., D.C., Former U.S. Senate Employee Sentenced to Prison Term on False Statements Charge (Dec. 20, 2018), https://tinyurl.com/bdz72dat ("[T]he FBI opened an investigation in April 2017 into the unauthorized disclosure of classified national security information that had appeared in a specific article published by a national news organization."); *see also* Press Release, U.S. Att'y's Off., D.C., Former U.S. Senate Employee Indicted on False Statements Charges (June 7, 2018), https://tinyurl.com/22xnmnx9.

Each aspect of this case was thus public by the time Empower Oversight sought the unsealing of the NDO applications. The only thing Empower Oversight did not know was how DOJ convinced the court to forbid disclosure of its collecting records of congressional staffers who were tasked with DOJ oversight. Because the investigation was "sufficiently widely known," even if the applications were Rule 6(e) materials at *some* point, they "lost [their] character as Rule 6(e) material" by the time Empower Oversight sought to unseal them. *In re North*, 16 F.3d at 1245.

The district court's error is only cemented by the Inspector General's report. Even if the public's knowledge of the investigation into the unauthorized disclosure of classification were up for debate when Empower Oversight first moved to unseal the NDO applications, that knowledge is now clear.

The Inspector General acknowledged details about the leak investigation and DOJ's seeking subpoenas for records about members of Congress and their staffers. That same report emphasized DOJ's attempts to keep those subpoenas secret, confirming that DOJ failed to inform Google or the court of the constitutional positions occupied by the

people whose phone numbers and email addresses appeared on the subpoena. It also confirmed that DOJ failed to provide any case-specific information, as required by DOJ policy and contemplated by the statute. With these details in the public domain, any plausible need for secrecy is gone. The "matters have already been publicly disclosed," and this Court should "unseal [the] records." *In re Cheney*, 2024 WL 1739096, at *3.

II. The First Amendment Right of Access to Judicial Records Applies to the NDO Applications.

In addition to the common-law right of access, Empower Oversight has a First Amendment right to the NDO applications. Although the Court need not reach this question, as the common-law right of access should be dispositive, *see Leopold II*, 964 F.3d at 1126–27 (not reaching the First Amendment right of access because the common-law right of access provided sufficient relief), the public's First Amendment right of access also requires disclosure of the NDO applications. Under the First Amendment, DOJ must satisfy strict scrutiny for the applications to remain sealed, which it cannot do.

A. Binding precedent confirms that the First Amendment requires disclosure.

To determine if the public has a First Amendment right of access to judicial documents, the Supreme Court applies an "experience and logic"

test. Under that test, the First Amendment is implicated when: (1) the types of judicial processes or records sought have historically been available to the public; and (2) public access plays a "significant positive role" in the functioning of those processes. *See Press-Enter. Co. v. Superior Court*, 478 U.S. 1, 9, 11 (1986); *Globe Newspaper Co. v. Superior Court*, 457 U.S. 596, 605–07 (1982); *Washington Post v. Robinson*, 935 F.2d 282, 287–92 (D.C. Cir. 1991); *United States v. Brice*, 649 F.3d 793, 795 (D.C. Cir. 2011) (applying the experience and logic test). Although this Court "has not resolved the question of whether the First Amendment right of access applies to" Stored Communications Act materials such as a § 2703(d) application or to the § 2705(b) NDO applications sought here, *In re N.Y. Times Co.*, No. 21-cv-0091-JEB, 2021 WL 5769444, at *8 (D.D.C. Dec. 6, 2021), both prongs support the public's First Amendment right of access to such documents.

1. There is a long tradition of public access to documents similar to the NDO applications.

Courts routinely provide public access to documents filed in connection with prior restraint proceedings or NDOs, as well as subpoenas, even where the information involves matters of national security. *See Doe v. Ashcroft*, 317 F. Supp. 2d 488, 491–93 (S.D.N.Y. 2004)

(ordering the parties to provide timely public access to all non-sensitive information filed in connection with a lawsuit challenging indefinite gag orders issued pursuant to 18 U.S.C. § 2709(c)); *In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 886 (S.D. Tex. 2008) ("The governmental interests considered here—the integrity of an ongoing criminal investigation, the reputational interests of targets, and the sensitivity of investigative techniques—are not sufficiently compelling to justify a permanent gag order.").

Similarly, courts in this Circuit have previously held that the First Amendment right of access applies to "warrant materials after an investigation has concluded," and that conclusion should apply with equal force to Stored Communications Act applications requesting forced non-disclosure of subpoenas under 18 U.S.C. § 2705(b). *Appl. of N.Y. Times*, 585 F. Supp. 2d at 88; *accord In re Appl. of WP Co. LLC*, No. 16-MC-351 (BAH), 2016 WL 1604976, at *2 (D.D.C. Apr. 1, 2016).

Moreover, as shown above, this Court in *Leopold II* held that the authority on which DOJ relied for the NDOs—18 U.S.C. §§ 2703(d) & 2705(b)—does not provide for automatic sealing. This stands in stark contrast to the automatic sealing afforded applications for judicial orders

in other contexts. *See* 15 U.S.C. § 57b-2a(e)(2) ("Upon application by the [Federal Trade] Commission, all judicial proceedings pursuant to this section [including proceedings under 18 U.S.C. § 2705(b)] shall be held in camera and the records thereof sealed until expiration of the period of delay or such other date as the presiding judge or magistrate judge may permit."); 18 U.S.C. § 2518(8)(b) ("Applications made and orders granted under this chapter [of the Wiretap Act] shall be sealed by the judge."). Through these statutes, Congress "demonstrate[ed] that it clearly understood how to" automatically displace the First Amendment right of access to judicial records "when it wished to do so." *Ysleta Del Sur Pueblo v. Texas*, 596 U.S. 685, 701 (2022). The lack of any such automatic sealing concerning the NDO applications sought here thus weighs strongly against automatic sealing or sealing beyond the term of the NDO, as that was clearly not Congress's intent.

2. Access to the NDO applications would prevent future executive abuses of process.

The logic prong of the test considers whether access to the sealed documents would serve a "significant positive role in the functioning of the particular process in question." *Press-Enter.*, 478 U.S. at 8 (citing *Globe Newspaper,* 457 U.S. at 606). This prong is clearly satisfied here

because the public is otherwise prevented from holding the government accountable when the government shields its own activities from public scrutiny. Indeed, transparency concerning judicial documents like the NDO applications would ensure fairness, decrease bias, improve public perception of the justice system, and enhance the chances that the resulting orders will be well-justified and narrowly tailored. *See Nixon*, 435 U.S. at 598 (explaining that the law's recognition of the importance of judicial transparency serves "the citizen's desire to keep a watchful eye on the workings of public agencies, and ... the operation of government"); *see also Appl. of N.Y. Times*, 585 F. Supp. 2d at 90 ("[W]ith respect to warrants, openness plays a significant positive role in the functioning of the criminal justice system, at least at the post-investigation stage.").

These interests are particularly acute where, as here, the government asserts authority affecting the First Amendment rights of a private actor—here, Google—that forbids it from communicating with others until the government allows the NDO to lapse, a classic prior restraint. *See Green v. U.S. Dep't of Just.*, 111 F.4th 81, 102 (D.C. Cir. 2024) (defining prior restraints as any regime that "require[s] prior governmental approval before a person may lawfully speak"). In short,

requiring DOJ to provide Empower Oversight with access to the NDO applications would provide the openness needed to ensure that the government is operating properly.

B. DOJ's attempts to keep the full NDO applications sealed cannot survive strict scrutiny.

Because the First Amendment right of access attaches to the NDO applications, DOJ's attempt to keep those applications under seal is subject to strict scrutiny. *See Globe Newspaper*, 457 U.S. at 606–07 & n.17. To overcome such scrutiny, DOJ must identify "compelling reasons," and the Court "must articulate specific findings on the record demonstrating that the decision to seal ... is narrowly tailored and essential to preserve [that] compelling government interest." *Robinson*, 935 F.2d at 289 & n.10; *see also Press-Enter.*, 478 U.S. at 15 ("The First Amendment right of access cannot be overcome by [a] conclusory assertion[.]").

1. Protecting the secrecy of a concluded criminal investigation that has been the subject of a public report from the Inspector General cannot qualify as a compelling governmental interest. *See Appl. of N.Y. Times*, 585 F. Supp. 2d at 90–92. That is especially true here, because the report conclusively found that none of the NDO applications or the follow-up

extension applications contained *any* case-specific information. OIG Rep. 4. There cannot be a compelling interest in keeping boilerplate applications secret.

Nor can DOJ claim an interest in preventing the public from learning that it sought to impose a prior restraint on Google to prevent Google from informing the targeted members of Congress and staffers that their communications records were collected. As the Supreme Court has explained, the protections against "prior restraint should have particular force as applied to reporting of criminal proceedings, whether the crime in question is a single isolated act or a pattern of criminal conduct." *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976). Those protections mean little if the government can hide behind sealed documents in perpetuity to avoid public inquiry.

2. Even if DOJ could demonstrate a compelling interest, its blanket sealing of all judicial documents remotely related to its investigation is not narrowly tailored to serve those interests, for at least two reasons. First, as the Fourth Circuit has recognized, the court must make individualized sealing determinations with respect to "each document" sought to be sealed. *See Stone v. Univ. of Md. Med. Sys. Corp.*, 855 F.2d

178, 181 (4th Cir. 1988) (noting that because different levels of protection attach to different judicial records, courts "must determine the source of the right of access with respect to each document sealed"). In other words, by failing to conduct a document-by-document review, DOJ has necessarily failed to narrowly tailor its sealing request.

Second, a document may not be sealed in its entirety if the government's interests can be accommodated through some "less drastic alternatives to sealing," such as redaction of specific information. *Id.*; *accord Appl. of N.Y. Times*, 585 F. Supp. 2d at 91 (holding that "the goal of protecting the confidentiality of informants can be accomplished by means less restrictive than prohibiting access to the warrant materials altogether"); *Appl. of WP Co.*, 2016 WL 1604976, at *2 ("While these interest[s] do not militate in favor of full secrecy, these interests may be protected through less restrictive means (i.e., redacting this information prior to unsealing the relevant materials)."). The Inspector General's finding that neither the original NDO applications nor the later extension requests contained *any* case-specific information underscores the lack of narrow tailoring. *See* OIG Rep. 4. And this means the district

court allowed DOJ to redact far too much when partially unsealing the NDO applications.

DOJ's continued efforts to keep the full boilerplate NDO applications secret cannot satisfy either prong of the strict-scrutiny analysis. This Court should thus reverse the district court's order allowing DOJ to redact the substance of the original and first extension applications. And it should reverse the district court's order denying Empower Oversight's motion in full as to all subsequent extension applications.

CONCLUSION

The district court applied the incorrect legal standard when denying Empower Oversight's request to unseal the NDO applications. The district court should have applied the common-law or First Amendment rights of access, each of which supports fully unsealing the NDO applications. Unsealing the NDO applications is vitally important for the public, as the recent Inspector General report confirms that DOJ failed to inform the district court that the underlying subpoenas sought communications records from members of Congress and congressional staff who were engaged in oversight of DOJ. The public has a keen

interest in understanding what exactly DOJ said to the court when attempting to justify its NDO applications.

Accordingly, the Court should reverse the district court and order DOJ to unseal the entirety of each NDO application.

Respectfully Submitted,

/s/ Brian J. Field
BRIAN J. FIELD
Counsel of Record
JOSHUA J. PRINCE
SCHAERR | JAFFE LLP
1717 K Street NW, Suite 900
Washington, DC 20006
(202) 787-1060
bfield@schaerr-jaffe.com

Counsel for Intervenor-Appellant

April 4, 2025

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing Brief of Intervenor-Appellant complies with the type-face requirements of Fed. R. App. P. 32(a)(5) & (6) and the 13,000-word type-volume limitation of Fed. R. App. P. 32(a)(7)(b) and 32(a)(7)(B) in that it uses Century Schoolbook 14-point type and contains 9,386 words, excluding the parts of the document exempted by Fed. R. App. P. 32(f). The number of words was determined through the word-count function of Microsoft Word.

s/ Brian J. Field
Brian J. Field

ADDENDA

INDEX

ADDENDUM A

18 U.S.C.A. § 2703

§ 2703. Required disclosure of customer communications or records

(a) Contents of wire or electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.--(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section;

except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service.--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) Requirement to preserve evidence.--

(1) In general.--A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.--Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) Presence of officer not required.--Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search

warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

(h) Comity analysis and disclosure of information regarding legal process seeking contents of wire or electronic communication.--

(1) Definitions.--In this subsection--

(A) the term "qualifying foreign government" means a foreign government--

(i) with which the United States has an executive agreement that has entered into force under section 2523; and

(ii) the laws of which provide to electronic communication service providers and remote computing service providers substantive and procedural opportunities similar to those provided under paragraphs (2) and (5); and

(B) the term "United States person" has the meaning given the term in section 2523.

(2) Motions to quash or modify.--(A) A provider of electronic communication service to the public or remote computing service, including a foreign electronic communication service or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes--

(i) that the customer or subscriber is not a United States person and does not reside in the United States; and

(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.

Such a motion shall be filed not later than 14 days after the date on which the provider was served with the legal process, absent agreement with the government or permission from the court to extend the deadline based on an application made within the 14 days. The right to move to quash is without prejudice to any other grounds to move to quash or defenses thereto, but it shall be the sole basis for moving to quash on the grounds of a conflict of law related to a qualifying foreign government.

(B) Upon receipt of a motion filed pursuant to subparagraph (A), the court shall afford the governmental entity that applied for or issued the legal process under this section the opportunity to respond. The court may modify or quash the legal process, as appropriate, only if the court finds that--

(i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;

(ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and

(iii) the customer or subscriber is not a United States person and does not reside in the United States.

(3) Comity analysis.--For purposes of making a determination under paragraph (2)(B)(ii), the court shall take into account, as appropriate--

(A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;

(B) the interests of the qualifying foreign government in preventing any prohibited disclosure;

(C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;

(D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country;

(E) the nature and extent of the provider's ties to and presence in the United States;

(F) the importance to the investigation of the information required to be disclosed;

(G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and

(H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.

(4) Disclosure obligations during pendency of challenge.--A service provider shall preserve, but not be obligated to produce, information sought during the pendency of a motion brought under this subsection, unless the court finds that

immediate production is necessary to prevent an adverse result identified in section 2705(a)(2).

(5) Disclosure to qualifying foreign government.--(A) It shall not constitute a violation of a protective order issued under section 2705 for a provider of electronic communication service to the public or remote computing service to disclose to the entity within a qualifying foreign government, designated in an executive agreement under section 2523, the fact of the existence of legal process issued under this section seeking the contents of a wire or electronic communication of a customer or subscriber who is a national or resident of the qualifying foreign government.

(B) Nothing in this paragraph shall be construed to modify or otherwise affect any other authority to make a motion to modify or quash a protective order issued under section 2705.

ADDENDUM B

18 U.S.C.A. § 2705

§ 2705. Delayed notice

(a) Delay of notification.--(1) A governmental entity acting under section 2703(b) of this title may--

(A) where a court order is sought, include in the application a request, which the court shall grant, for an order delaying the notification required under section 2703(b) of this title for a period not to exceed ninety days, if the court determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2) of this subsection; or

(B) where an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury subpoena is obtained, delay the notification required under section 2703(b) of this title for a period not to exceed ninety days upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2) of this subsection.

(2) An adverse result for the purposes of paragraph (1) of this subsection is--

(A) endangering the life or physical safety of an individual;

(B) flight from prosecution;

(C) destruction of or tampering with evidence;

(D) intimidation of potential witnesses; or

(E) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The governmental entity shall maintain a true copy of certification under paragraph (1)(B).

(4) Extensions of the delay of notification provided in section 2703 of up to ninety days each may be granted by the court upon application, or by certification by a governmental entity, but only in accordance with subsection (b) of this section.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4) of this subsection, the governmental entity shall serve upon, or deliver by registered or first-class mail to, the customer or subscriber a copy of the process or request together with notice that--

(A) states with reasonable specificity the nature of the law enforcement inquiry; and

(B) informs such customer or subscriber--

(i) that information maintained for such customer or subscriber by the service provider named in such process or request was supplied to or requested by that governmental authority and the date on which the supplying or request took place;

(ii) that notification of such customer or subscriber was delayed;

(iii) what governmental entity or court made the certification or determination pursuant to which that delay was made; and

(iv) which provision of this chapter allowed such delay.

(6) As used in this subsection, the term "supervisory official" means the investigative agent in charge or assistant investigative agent in charge or an equivalent of an investigating agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney or an equivalent of a prosecuting attorney's headquarters or regional office.

(b) Preclusion of notice to subject of governmental access.--A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in--

(1) endangering the life or physical safety of an individual;

(2) flight from prosecution;

(3) destruction of or tampering with evidence;

(4) intimidation of potential witnesses; or

(5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

ADDENDUM C

Federal Rules of Criminal Procedure, Rule 6

Rule 6. The Grand Jury

(a) Summoning a Grand Jury.

(1) In General. When the public interest so requires, the court must order that one or more grand juries be summoned. A grand jury must have 16 to 23 members, and the court must order that enough legally qualified persons be summoned to meet this requirement.

(2) Alternate Jurors. When a grand jury is selected, the court may also select alternate jurors. Alternate jurors must have the same qualifications and be selected in the same manner as any other juror. Alternate jurors replace jurors in the same sequence in which the alternates were selected. An alternate juror who replaces a juror is subject to the same challenges, takes the same oath, and has the same authority as the other jurors.

(b) Objection to the Grand Jury or to a Grand Juror.

(1) Challenges. Either the government or a defendant may challenge the grand jury on the ground that it was not lawfully drawn, summoned, or selected, and may challenge an individual juror on the ground that the juror is not legally qualified.

(2) Motion to Dismiss an Indictment. A party may move to dismiss the indictment based on an objection to the grand jury or on an individual juror's lack of legal qualification, unless the court has previously ruled on the same objection under Rule 6(b)(1). The motion to dismiss is governed by 28 U.S.C. § 1867(e). The court must not dismiss the indictment on the ground that a grand juror was not legally qualified if the record shows that at least 12 qualified jurors concurred in the indictment.

(c) Foreperson and Deputy Foreperson. The court will appoint one juror as the foreperson and another as the deputy foreperson. In the foreperson's absence, the deputy foreperson will act as the foreperson. The foreperson may administer oaths and affirmations and will sign all indictments. The foreperson--or another juror designated by the foreperson--will record the number of jurors concurring in every indictment and will file the record with the clerk, but the record may not be made public unless the court so orders.

(d) Who May Be Present.

(1) While the Grand Jury Is in Session. The following persons may be present while the grand jury is in session: attorneys for the government, the witness being

questioned, interpreters when needed, and a court reporter or an operator of a recording device.

(2) During Deliberations and Voting. No person other than the jurors, and any interpreter needed to assist a hearing-impaired or speech-impaired juror, may be present while the grand jury is deliberating or voting.

(e) Recording and Disclosing the Proceedings.

(1) Recording the Proceedings. Except while the grand jury is deliberating or voting, all proceedings must be recorded by a court reporter or by a suitable recording device. But the validity of a prosecution is not affected by the unintentional failure to make a recording. Unless the court orders otherwise, an attorney for the government will retain control of the recording, the reporter's notes, and any transcript prepared from those notes.

(2) Secrecy.

(A) No obligation of secrecy may be imposed on any person except in accordance with Rule 6(e)(2)(B).

(B) Unless these rules provide otherwise, the following persons must not disclose a matter occurring before the grand jury:

(i) a grand juror;

(ii) an interpreter;

(iii) a court reporter;

(iv) an operator of a recording device;

(v) a person who transcribes recorded testimony;

(vi) an attorney for the government; or

(vii) a person to whom disclosure is made under Rule 6(e)(3)(A)(ii) or (iii).

(3) Exceptions.

(A) Disclosure of a grand-jury matter--other than the grand jury's deliberations or any grand juror's vote--may be made to:

(i) an attorney for the government for use in performing that attorney's duty;

(ii) any government personnel--including those of a state, state subdivision, Indian tribe, or foreign government--that an attorney for the government considers necessary to assist in performing that attorney's duty to enforce federal criminal law; or

(iii) a person authorized by 18 U.S.C. § 3322.

(B) A person to whom information is disclosed under Rule 6(e)(3)(A)(ii) may use that information only to assist an attorney for the government in performing that attorney's duty to enforce federal criminal law. An attorney for the government must promptly provide the court that impaneled the grand jury with the names of all persons to whom a disclosure has been made, and must certify that the attorney has advised those persons of their obligation of secrecy under this rule.

(C) An attorney for the government may disclose any grand-jury matter to another federal grand jury.

(D) An attorney for the government may disclose any grand-jury matter involving foreign intelligence, counterintelligence (as defined in 50 U.S.C. § 3003), or foreign intelligence information (as defined in Rule 6(e)(3)(D)(iii)) to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official to assist the official receiving the information in the performance of that official's duties. An attorney for the government may also disclose any grand-jury matter involving, within the United States or elsewhere, a threat of attack or other grave hostile acts of a foreign power or its agent, a threat of domestic or international sabotage or terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by its agent, to any appropriate federal, state, state subdivision, Indian tribal, or foreign government official, for the purpose of preventing or responding to such threat or activities.

(i) Any official who receives information under Rule 6(e)(3)(D) may use the information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information. Any state, state subdivision, Indian tribal, or foreign government official who receives information under Rule 6(e)(3)(D) may use the information only in a manner consistent with any guidelines issued by the Attorney General and the Director of National Intelligence.

(ii) Within a reasonable time after disclosure is made under Rule 6(e)(3)(D), an attorney for the government must file, under seal, a notice with the court in the district where the grand jury convened stating that such information was disclosed and the departments, agencies, or entities to which the disclosure was made.

(iii) As used in Rule 6(e)(3)(D), the term “foreign intelligence information” means:

(a) information, whether or not it concerns a United States person, that relates to the ability of the United States to protect against--

• actual or potential attack or other grave hostile acts of a foreign power or its agent;

• sabotage or international terrorism by a foreign power or its agent; or

• clandestine intelligence activities by an intelligence service or network of a foreign power or by its agent; or

(b) information, whether or not it concerns a United States person, with respect to a foreign power or foreign territory that relates to--

• the national defense or the security of the United States; or

• the conduct of the foreign affairs of the United States.

(E) The court may authorize disclosure--at a time, in a manner, and subject to any other conditions that it directs--of a grand-jury matter:

(i) preliminarily to or in connection with a judicial proceeding;

(ii) at the request of a defendant who shows that a ground may exist to dismiss the indictment because of a matter that occurred before the grand jury;

(iii) at the request of the government, when sought by a foreign court or prosecutor for use in an official criminal investigation;

(iv) at the request of the government if it shows that the matter may disclose a violation of State, Indian tribal, or foreign criminal law, as long as the disclosure is to an appropriate state, state-subdivision, Indian tribal, or foreign government official for the purpose of enforcing that law; or

(v) at the request of the government if it shows that the matter may disclose a violation of military criminal law under the Uniform Code of Military Justice, as long as the disclosure is to an appropriate military official for the purpose of enforcing that law.

(F) A petition to disclose a grand-jury matter under Rule 6(e)(3)(E)(i) must be filed in the district where the grand jury convened. Unless the hearing is ex parte--as it may be when the government is the petitioner--the petitioner must serve the petition on, and the court must afford a reasonable opportunity to appear and be heard to:

(i) an attorney for the government;

(ii) the parties to the judicial proceeding; and

(iii) any other person whom the court may designate.

(G) If the petition to disclose arises out of a judicial proceeding in another district, the petitioned court must transfer the petition to the other court unless the petitioned court can reasonably determine whether disclosure is proper. If the

petitioned court decides to transfer, it must send to the transferee court the material sought to be disclosed, if feasible, and a written evaluation of the need for continued grand-jury secrecy. The transferee court must afford those persons identified in Rule 6(e)(3)(F) a reasonable opportunity to appear and be heard.

(4) Sealed Indictment. The magistrate judge to whom an indictment is returned may direct that the indictment be kept secret until the defendant is in custody or has been released pending trial. The clerk must then seal the indictment, and no person may disclose the indictment's existence except as necessary to issue or execute a warrant or summons.

(5) Closed Hearing. Subject to any right to an open hearing in a contempt proceeding, the court must close any hearing to the extent necessary to prevent disclosure of a matter occurring before a grand jury.

(6) Sealed Records. Records, orders, and subpoenas relating to grand-jury proceedings must be kept under seal to the extent and as long as necessary to prevent the unauthorized disclosure of a matter occurring before a grand jury.

(7) Contempt. A knowing violation of Rule 6, or of any guidelines jointly issued by the Attorney General and the Director of National Intelligence under Rule 6, may be punished as a contempt of court.

(f) Indictment and Return. A grand jury may indict only if at least 12 jurors concur. The grand jury--or its foreperson or deputy foreperson--must return the indictment to a magistrate judge in open court. To avoid unnecessary cost or delay, the magistrate judge may take the return by video teleconference from the court where the grand jury sits. If a complaint or information is pending against the defendant and 12 jurors do not concur in the indictment, the foreperson must promptly and in writing report the lack of concurrence to the magistrate judge.

(g) Discharging the Grand Jury. A grand jury must serve until the court discharges it, but it may serve more than 18 months only if the court, having determined that an extension is in the public interest, extends the grand jury's service. An extension may be granted for no more than 6 months, except as otherwise provided by statute.

(h) Excusing a Juror. At any time, for good cause, the court may excuse a juror either temporarily or permanently, and if permanently, the court may impanel an alternate juror in place of the excused juror.

(i) "Indian Tribe" Defined. "Indian tribe" means an Indian tribe recognized by the Secretary of the Interior on a list published in the Federal Register under 25 U.S.C. § 479a-1.[1]

---

[1] Editorially reclassified as 25 U.S.C. § 5131.